Bull. Aust. Math. Soc. **89** (2014), 300–307
doi:10.1017/S0004972713000671

ON SOLUTIONS TO SOME POLYNOMIAL CONGRUENCES IN SMALL BOXES

IGOR E. SHPARLINSKI

(Received 21 March 2013; accepted 15 June 2013; first published online 7 August 2013)

Abstract

We use bounds of mixed character sum to study the distribution of solutions to certain polynomial systems of congruences modulo a prime p. In particular, we obtain nontrivial results about the number of solutions in boxes with the side length below $p^{1/2}$, which seems to be the limit of more general methods based on the bounds of exponential sums along varieties.

2010 *Mathematics subject classification*: primary 11D79; secondary 11K38.
Keywords and phrases: multivariate congruences, distribution of points.

1. Introduction

There is an extensive literature investigating the distribution of solutions to the system of congruences

$$F_j(x_1, \dots, x_n) \equiv 0 \pmod p, \qquad j = 1, \dots, m, \tag{1.1}$$

with polynomials $F_j(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$, $j = 1, \dots, m$, in m variables with integer coefficients, modulo a prime p; see [4, 5, 8, 11, 12].

In particular, subject to some additional condition (related to the so-called A-number), Fouvry and Katz [5, Corollary 1.5] have given an asymptotic formula for the number of solutions to (1.1) in a box

$$(x_1, \dots, x_n) \in [0, h-1]^n$$

for a rather small h. In fact, the limit of the method of [5] is $h = p^{1/2+o(1)}$.

Here we consider a very special class of systems of $s+1$ polynomial congruences

$$x_1 \cdots x_n \equiv a \pmod p, \tag{1.2}$$

and

$$c_{1,j}x_1^{k_{1,j}} + \cdots + c_{n,j}x_n^{k_{m,j}} \equiv b_j \pmod p, \qquad j = 1, \dots, s, \tag{1.3}$$

This work was supported in part by the ARC Grant DP130100237.

where $a, b_j, c_{i,j}, k_{i,j} \in \mathbb{Z}$, with $\gcd(ac_{i,j}, p) = 1$, $i = 1, \ldots, n$, $j = 1, \ldots, s$, and $3 \le k_{i,1} < \cdots < k_{i,s}$.

The interest in the systems of congruences (1.2) and (1.3) stems from the work of Fouvry and Katz [5], where a particular case of the congruence (1.2) and just one congruence of the type (1.3) (that is, for $s = 1$) with the same odd exponents $k_{1,1} = \cdots = k_{n,1} = k$ and $b_1 = 0$ is given as an example of a variety to which one of their main general results applies. In particular, in this case and for $k \ge 3$, $b_1 = 0$ (and fixed nonzero coefficients) we see that [5, Theorem 1.5] gives an asymptotic for the number of solutions with $1 \le x_i \le h$, $i = 1, \ldots, n$, starting from the values of h of size about $\max\{p^{1/2+1/n}, p^{3/4}\} \log p$. Here we show that a different and more specialised treatment allows a significant lowering of this threshold, which now in some cases reaches $p^{1/4+\kappa}$ for any $\kappa > 0$. Furthermore, this applies to the systems (1.2) and (1.3) in full generality and is uniform with respect to the coefficients.

More precisely, we use a combination of:

- the bound of mixed character sums to due to Chang [3];
- the result of Ayyad *et al.* [1] on the fourth moment of short character sums;
- the bound of Wooley [14] on exponential sums with polynomials.

We note that the classical Pólya–Vinogradov and Burgess bounds of multiplicative character sums (see [6, Theorems 12.5 and 12.6]), in combination with a result of Ayyad *et al.* [1], have been used in [9, 10] to study the distribution of the single congruence (1.2) in very small boxes, and thus go below the $p^{1/2}$-threshold.

Here we show that the recent result of Chang [3] enables us now to study a much more general case of the simultaneous congruences (1.2) and (1.3).

Throughout the paper, the implied constants in the symbols O and $\ll$ can depend on the positive parameter κ and on the degrees $k_{i,j}$ in (1.2) and (1.3) as well as, occasionally, of some other polynomials involved. We recall that the expressions $A \ll B$ and $A = O(B)$ are each equivalent to the statement that $|A| \le cB$ for some constant c.

2. Character and exponential sums

Let $\mathcal{X}_p$ be the set of multiplicative characters modulo p and let $\mathcal{X}_p^* = \mathcal{X}_p \setminus \{\chi_0\}$ be the set of nonprincipal characters. We also write

$$\mathbf{e}_p(z) = \exp(2\pi i z/p).$$

We appeal to [6] for a background on the basic properties of multiplicative characters and exponential functions, such as orthogonality.

The following bounds of exponential sums twisted with a multiplicative character have been given by Chang [3] for sums in arbitrary finite fields but only for intervals starting at the origin. However, a simple examination of the argument of [3] reveals that this is not important for the proof.

https://doi.org/10.1017/S0004972713000671 Published online by Cambridge University Press

Lemma 2.1. *For any character $\chi \in \mathcal{X}_p^*$, a polynomial $F(X) \in \mathbb{Z}[X]$ of degree k and integers u and $h \ge p^{1/4+\kappa}$,*

$$\sum_{x=u+1}^{u+h} \chi(x)\mathbf{e}_p(F(x)) \ll hp^{-\eta},$$

where

$$\eta = \frac{\kappa^2}{4(1+2\kappa)(k^2+2k+3)}.$$

We note that we do not impose any conditions on the polynomial F in Lemma 2.1.

On the other hand, when $\chi = \chi_0$, we use the following very special case of the much more general bound of Wooley [14] that applies to polynomials with arbitrary real coefficients.

Lemma 2.2. *For any polynomial $F(X) \in \mathbb{Z}[X]$ of degree $k > 2$ with the leading coefficient $a_k \not\equiv 0 \pmod p$, and any integers u and h with $h < p$,*

$$\sum_{x=u+1}^{u+h} \mathbf{e}_p(F(x)) \ll h^{1-1/2k(k-2)} + h^{1-1/2(k-2)}p^{1/2k(k-2)}.$$

Clearly, Lemma 2.2 is nontrivial only for $h \ge p^{1/k}$, which is actually the best possible range. Furthermore, in a slightly shorter range we have the following corollary.

Corollary 2.3. *For any polynomial $F(X) \in \mathbb{Z}[X]$ of degree $k > 2$ with the leading coefficient $a_k \not\equiv 0 \pmod p$, and any integers u and h with $p^{1/(k-1)} \le h < p$,*

$$\sum_{x=u+1}^{u+h} \mathbf{e}_p(F(x)) \ll h^{1-1/2k(k-2)}.$$

We make use of the following estimate of Ayyad *et al.* [1, Theorem 1].

Lemma 2.4. *Uniformly over integers u and $h \le p$, the congruence*

$$x_1x_2 \equiv x_3x_4 \pmod p, \qquad u+1 \le x_1, x_2, x_3, x_4 \le u+h,$$

has $h^4/p + O(h^2p^{o(1)})$ solutions as $h \to \infty$.

We note that Lemma 2.4 is a essentially a statement about the fourth moment of short character sums; see [1, Equation (4)]. In fact, the next result makes it clearer.

Corollary 2.5. *Let $\rho(x)$ be an arbitrary complex valued function with*

$$|\rho(x)| \le 1, \qquad x \in \mathbb{R}.$$

https://doi.org/10.1017/S0004972713000671 Published online by Cambridge University Press

Uniformly over integers $1 \le u \le u + h < p$,

$$\sum_{\chi \in \mathcal{X}_p} \Big| \sum_{x=u+1}^{u+h} \rho(x)\chi(x) \Big|^4 \le h^4 + O(h^2 p^{1+o(1)}),$$

as $h \to \infty$.

Proof. Expanding the fourth power and changing the order of summation,

$$\begin{aligned} \sum_{\chi \in \mathcal{X}_p} \Big| \sum_{x=u_i+1}^{u+h} \rho(x)\chi(x) \Big|^4 &= \sum_{\chi \in \mathcal{X}_p} \sum_{x_1,\dots,x_4=u+1}^{u+h} \rho(x_1)\rho(x_2)\overline{\rho}(x_3)\overline{\rho}(x_4)\chi(x_1x_2x_3^{-1}x_4^{-1}) \\ &= \sum_{x_1,\dots,x_4=u+1}^{u+h} \rho(x_1)\rho(x_2)\overline{\rho}(x_3)\overline{\rho}(x_4) \sum_{\chi \in \mathcal{X}_p} \chi(x_1x_2x_3^{-1}x_4^{-1}). \end{aligned}$$

Using the orthogonality of characters, we write

$$\begin{aligned} \sum_{\chi \in \mathcal{X}_p} \Big| \sum_{x=u+1}^{u+h} \rho(x)\chi(x) \Big|^4 &= (p-1) \sum_{\substack{x_1,\dots,x_4=u+1 \\ x_1x_2 \equiv x_3x_4 \pmod p}}^{u+h} \rho(x_1)\rho(x_2)\overline{\rho}(x_3)\overline{\rho}(x_4) \\ &\le (p-1) \sum_{\substack{x_1,\dots,x_4=u+1 \\ x_1x_2 \equiv x_3x_4 \pmod p}}^{u+h} 1. \end{aligned}$$

Applying Lemma 2.4, we derive the desired bound. □

3. Main result

We are now able to present our main result. Let $\mathfrak{B}$ be a cube of the form

$$\mathfrak{B} = [u_1 + 1, u_1 + h] \times \cdots \times [u_n + 1, u_n + h]$$

with some integers h, u_i with $1 \le u_i + 1 < u_i + h < p$, $i = 1, \dots, n$. We denote by $N(\mathfrak{B})$ the number of integer vectors

$$(x_1, \dots, x_n) \in \mathfrak{B}$$

satisfying (1.2) and (1.3) simultaneously.

As we have mentioned, the case of just one congruence (1.2) has been considered in [9, 10], so we always assume that $s \ge 1$ (and thus $n \ge 3$).

Let

$$\begin{aligned} k &= \min\{k_{i,j} \ : \ i = 1, \dots, n, \ \ j = 1, \dots, s\}, \\ K &= \max\{k_{i,j} \ : \ i = 1, \dots, n, \ \ j = 1, \dots, s\}. \end{aligned}$$

Recall that, due to our assumption, $K \ge k \ge 3$.

THEOREM 3.1. *For any fixed $\kappa > 0$ and*

$$p > h \geq \min\{p^{1/4+\kappa}, p^{1/(k-1)}\}$$

we have

$$N_p(\mathfrak{B}) = \frac{h^n}{p^{s+1}} + O(h^n p^{-1-\eta(n-4)} + h^{n-2} p^{-\eta(n-4)}),$$

where

$$\eta = \frac{\kappa^2}{4(1+2\kappa)(K^2+2K+3)}.$$

PROOF. Using the orthogonality of characters, we write

$$N_p(\mathfrak{B}) = \sum_{(x_1,\ldots,x_n)\in\mathfrak{B}} \frac{1}{p^s} \sum_{\lambda_1,\ldots,\lambda_s=0}^{p-1} \mathbf{e}_p\bigg(\sum_{j=1}^{s} \lambda_j\bigg(\sum_{i=1}^{n} c_{i,j} x_i^{k_{i,j}} - b_j\bigg)\bigg)$$
$$\times \frac{1}{p-1} \sum_{\chi\in\mathcal{X}_p} \chi(x_1 \cdots x_n a^{-1}).$$

Hence, changing the order of summation,

$$N_p(\mathfrak{B}) = \frac{1}{(p-1)p^s} \sum_{\lambda_1,\ldots,\lambda_s=0}^{p-1} \mathbf{e}_p\bigg(-\sum_{j=1}^{s} \lambda_j b_j\bigg) \sum_{\chi\in\mathcal{X}_p} \chi(a^{-1}) \prod_{i=1}^{n} S_i(\chi; \lambda_1, \ldots, \lambda_s),$$

where

$$S_i(\chi; \lambda_1, \ldots, \lambda_s) = \sum_{x=u_i+1}^{u_i+h} \chi(x) \mathbf{e}_p\bigg(\sum_{j=1}^{s} \lambda_j c_{i,j} x^{k_{i,j}}\bigg), \quad i = 1, \ldots, n.$$

Separating the term $h^n/(p-1)p^s$, corresponding to $\chi = \chi_0$ and $\lambda_1 = \cdots = \lambda_s = 0$, we derive

$$N_p(\mathfrak{B}) - \frac{h^n}{(p-1)p^s} \ll \frac{1}{p^{s+1}}(R_1 + R_2), \tag{3.1}$$

where

$$R_1 = \sum_{\lambda_1,\ldots,\lambda_s=0}^{p-1} \sum_{\chi\in\mathcal{X}_p^*} \prod_{i=1}^{n} |S_i(\chi; \lambda_1, \ldots, \lambda_s)|,$$

$$R_2 = \sum_{\substack{\lambda_1,\ldots,\lambda_s=0\\(\lambda_1,\ldots,\lambda_s)\neq(0,\ldots,0)}}^{p-1} \prod_{i=1}^{n} |S_i(\chi_0; \lambda_1, \ldots, \lambda_s)|.$$

To estimate R_1, we use Lemma 2.1 and write

$$R_1 \leq h^{n-4} p^{-\eta(n-4)} \sum_{\lambda_1,\ldots,\lambda_s=0}^{p-1} \sum_{\chi\in\mathcal{X}_p^*} \prod_{i=1}^{4} |S_i(\chi; \lambda_1, \ldots, \lambda_s)|.$$

https://doi.org/10.1017/S0004972713000671 Published online by Cambridge University Press

Using the Hölder inequality and Corollary 2.5,

$$\sum_{\chi\in\mathcal{X}_p^*}\prod_{i=1}^{4}|S_i(\chi;\lambda_1,\ldots,\lambda_s)| \le \Big(\prod_{i=1}^{4}\sum_{\chi\in\mathcal{X}_p^*}|S_i(\chi;\lambda_1,\ldots,\lambda_s)|^4\Big)^{1/4}$$
$$\ll h^4+h^2p^{1+o(1)}.$$

Therefore,

$$R_1 \ll h^n p^{s-\eta(n-4)} + h^{n-2}p^{s+1-\eta(n-4)}. \tag{3.2}$$

Furthermore, for R_2 we use Corollary 2.3 to derive

$$R_2 \le h^{(n-2)(1-1/2K(K-2))}\sum_{\substack{\lambda_1,\ldots,\lambda_s=0\\(\lambda_1,\ldots,\lambda_s)\neq(0,\ldots,0)}}^{p-1}\prod_{i=1}^{2}|S_i(\chi_0;\lambda_1,\ldots,\lambda_s)|.$$

Using the Hölder inequality and the orthogonality of exponential functions (similarly to the proof of Corollary 2.5),

$$\sum_{\substack{\lambda_1,\ldots,\lambda_s=0\\(\lambda_1,\ldots,\lambda_s)\neq(0,\ldots,0)}}^{p-1}\prod_{i=1}^{2}|S_i(\chi_0;\lambda_1,\ldots,\lambda_s)| \le \Big(\prod_{i=1}^{2}\sum_{\lambda_1,\ldots,\lambda_s=0}^{p-1}|S_i(\chi_0;\lambda_1,\ldots,\lambda_s)|^2\Big)^{1/2} \ll p^s h.$$

Thus

$$R_2 \ll h^{n-1-(n-2)/2K(K-2)}p^s. \tag{3.3}$$

Substituting the bounds (3.2) and (3.3) in (3.1),

$$N_p(\mathfrak{B})-\frac{h^n}{p^{s+1}} \ll h^n p^{-1-\eta(n-4)} + h^{n-2}p^{-\eta(n-4)} + h^{n-1-(n-2)/2K(K-2)}p^{-1}.$$

Clearly,

$$4\eta < \frac{1}{2K(K-2)}.$$

Thus we see that

$$p^{\eta(n-4)} < h^{4\eta(n-4)} < h^{(n-2)/2K(K-2)}.$$

Hence the second term always dominates the third term and the result follows. □

4. Comments

Clearly, for any $\kappa>0$, $k\ge 5$ and $p>h\ge p^{1/4+\kappa}$, Theorem 3.1 implies that

$$N_p(\mathfrak{B}) = (1+o(1))\frac{h^n}{p^{s+1}},$$

as $p\to\infty$, provided that

$$n \ge (s+1/2)\eta^{-1}+4.$$

https://doi.org/10.1017/S0004972713000671 Published online by Cambridge University Press

For $k = 3$ and 4 the range of Theorem 3.1 becomes $h \ge p^{1/2}$ and $h \ge p^{1/3}$, respectively. However, it is easy to see that using the full power of Lemma 2.2 instead of Corollary 2.3 one can derive nontrivial results in a wider range. Namely, for any $\kappa > 0$ there exists some $\gamma > 0$ (independent of n and other parameters in (1.2) and (1.3)) such that, for $h \ge p^{1/3+\kappa}$ if $k = 3$ and for $h \ge p^{1/4+\kappa}$ if $k = 4$,

$$N_p(\mathfrak{B}) = \frac{h^n}{(p-1)p^s} + O(h^{(1-\gamma)n}).$$

We also recall that for polynomials of small degrees stronger versions of Lemma 2.2 are available; see [2] and references therein.

Note that the same method can be applied (with essentially the same results) to the systems of congruences where instead of (1.2) we have a more general congruence

$$x_1^{m_1} \cdots x_n^{m_n} \equiv a \pmod p$$

for some integers m_i with $\gcd(m_i, p-1) = 1$, $i = 1, \ldots, n$.

Moreover, we recall that the Weil bound [13, Appendix 5, Example 12] (see also [7, Ch. 6, Theorem 3]) and the standard reduction between complete and incomplete sums (see [6, Section 12.2]) imply that

$$\sum_{x=u+1}^{u+h} \chi(G(x))\mathbf{e}_p(F(x)) \ll p^{1/2} \log p,$$

where $G(x)$ is a polynomial that is not a perfect power of any other polynomial in the algebraic closure $\overline{\mathbb{F}}_p$ of the finite field of p elements. Thus for $h \ge p^{1/2+\kappa}$, using this bound instead of Lemma 2.1 allows us to replace (1.2) with the congruence

$$G_1(x_1) \cdots G_n(x_n) \equiv a \pmod p$$

for arbitrary polynomials $G_1(X), \ldots, G_n(X) \in \mathbb{Z}[X]$ such that their reductions modulo p are not perfect powers in $\overline{\mathbb{F}}_p$. In fact, even for $G_1(X) = \cdots = G_n(X) = X$ (that is, for the congruence (1.2)) this leads to a result which is sometimes stronger that those of [5] and Theorem 3.1.

Acknowledgement

The author is very grateful to Mei-Chu Chang for the confirmation that the main result of [3] applies to intervals in an arbitrary position.

References

[1] A. Ayyad, T. Cochrane and Z. Zheng, 'The congruence $x_1x_2 \equiv x_3x_4 (\mathrm{mod}\ p)$, the equation $x_1x_2 = x_3x_4$ and the mean value of character sums', *J. Number Theory* **59** (1996), 398–413.

[2] K. D. Boklan and T. D. Wooley, 'On Weyl sums for smaller exponents', *Funct. Approx. Comment. Math.* **46** (2012), 91–107.

https://doi.org/10.1017/S0004972713000671 Published online by Cambridge University Press

[3] M.-C. Chang, ‘An estimate of incomplete mixed character sums’, in: *An Irregular Mind*, Bolyai Society Mathematical Studies, 21 (Springer, Berlin, 2010), 243–250.

[4] É. Fouvry, ‘Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums’, *Israel J. Math.* **120** (2000), 81–96.

[5] É. Fouvry and N. Katz, ‘A general stratification theorem for exponential sums, and applications’, *J. reine angew. Math.* **540** (2001), 115–166.

[6] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (American Mathematical Society, Providence, RI, 2004).

[7] W.-C. W. Li, *Number Theory with Applications* (World Scientific, Singapore, 1996).

[8] W. Luo, ‘Rational points on complete intersections over $\mathbb{F}_p$’, *Int. Math. Res. Not. IMRN* **1999** (1999), 901–907.

[9] I. E. Shparlinski, ‘On the distribution of points on multidimensional modular hyperbolas’, *Proc. Japan Acad. Ser. A Math. Sci.* **83** (2007), 5–9.

[10] I. E. Shparlinski, ‘On a generalisation of a Lehmer problem’, *Math. Z.* **263** (2009), 619–631.

[11] I. E. Shparlinski and A. N. Skorobogatov, ‘Exponential sums and rational points on complete intersections’, *Mathematika* **37** (1990), 201–208.

[12] A. N. Skorobogatov, ‘Exponential sums, the geometry of hyperplane sections, and some Diophantine problems’, *Israel J. Math.* **80** (1992), 359–379.

[13] A. Weil, *Basic Number Theory* (Springer, New York, 1974).

[14] T. D. Wooley, ‘Vinogradov’s mean value theorem via efficient congruencing, II’, *Duke Math. J.* **162**(4) (2013), 673–730.

IGOR E. SHPARLINSKI, Department of Computing,
Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor.shparlinski@mq.edu.au

https://doi.org/10.1017/S0004972713000671 Published online by Cambridge University Press